Security in the Cloud

Visibility & Control of your Cloud Service Provider

Prashant Haldankar, Pierre Tagle Ph.D.
AusCERT 2012

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney
Level 8, 66 King Street
Sydney NSW 2000
Australia

Melbourne
Level 10, 401 Docklands Drv
Docklands VIC 3008
Australia

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

Outline

- Cloud Service Providers and Security
- Developing a Strategic Cloud Security Roadmap
- Questions to Ask a CSP - make an informed decision

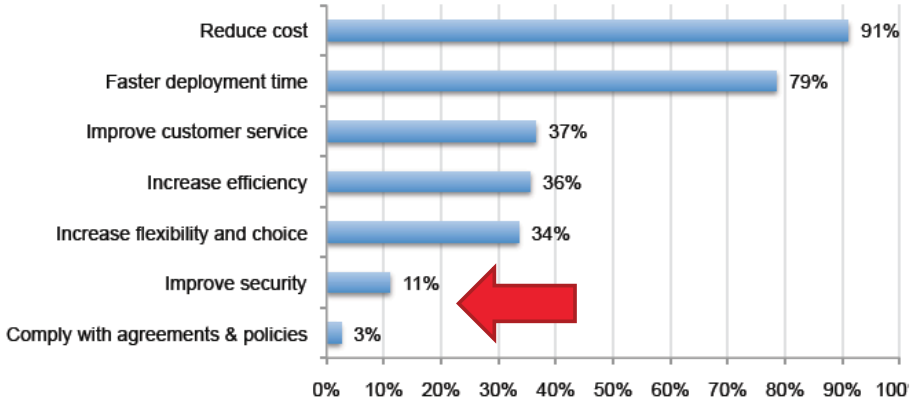
Introduction

- Looking to the cloud
  - Gartner says that in 2012, 80% of Fortune 1000 enterprises will pay for cloud services
  - Another 30% will pay for cloud infrastructure

- Cloud summary
  - Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)
  - Cloud Service Provider (CSP)

Customers and the Cloud

- Cloud service providers (CSP) do not think security is a reason for customers to use their services.
- The top choices are reduced cost, faster deployment time, improved customer service, and increased efficiency.



Source: "Security of Cloud Computing Providers Study", Ponemon Institute (April 2011)

Cloud Security Risks

- Areas cloud providers are most confident:
  - ability to ensure recovery from significant IT failures
  - ensure physical location of data assets are in secure environment

Source: "Security of Cloud Computing Providers Study", Ponemon Institute (April 2011)

- Areas cloud providers are least confident:
  - ability to restrict privileged user access to sensitive data
  - ensure proper data segregation requirements are met

Other CSP Findings

- Majority of CSPs believe it is the customer's responsibility to secure the cloud.
- Majority say their systems and applications are not always evaluated for security threats prior to deployment to customers.
- Majority of CSPs in the study admit they do not have dedicated security personnel
- Different priorities between users and CSPs with regards to critical security areas

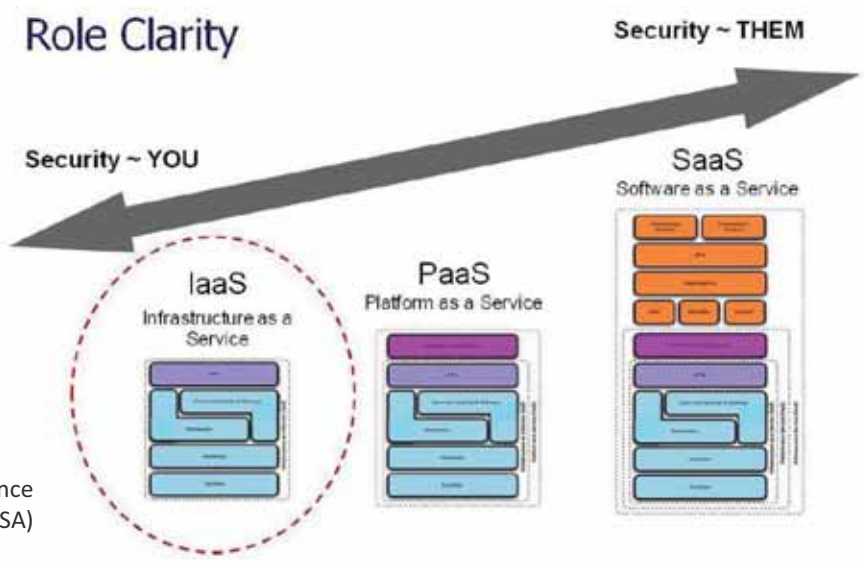
Who is most responsible for ensuring the security of cloud resources by cloud providers?

Critical areas of security for cloud providers

Source: "Security of Cloud Computing Providers Study", Ponemon Institute (April 2011)

Cloud Service Models

Differences in scope and control among cloud service models (cloud provider vs. consumer)



Source: Cloud Security Alliance (CSA)

Service Agreements

- Service agreements
  - Terms & conditions of access
  - Use of services
  - Service period, exit conditions
- Pre-defined non-negotiable agreements vs. negotiated agreements
  - Pre-defined: prescribed by CSP, not written to align with regulations, unilateral changes, basis for economies of scale
  - Negotiated: can be used to address specific concerns, normally more costly

Cloud Security Roadmap

Developing a strategic cloud security roadmap

- Define business & IT strategy
- Define GRC strategy
- Identify the risks
- Choose / select providers
- Document the plan

Define Business & IT Strategy

- Business-centric security
  - Understand the business requirements
  - Define appropriate policies
- Data sensitivity
  - Low, medium & high sensitivity
  - Cross border questions
- Risk appetite
  - Will direct the scope & depth of cloud services
  - Business agreement on acceptable risk

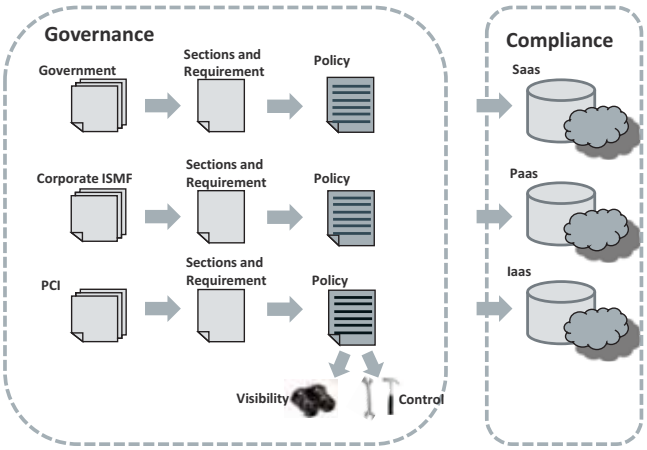
Define GRC Strategy

Survivability & Legal Strategy

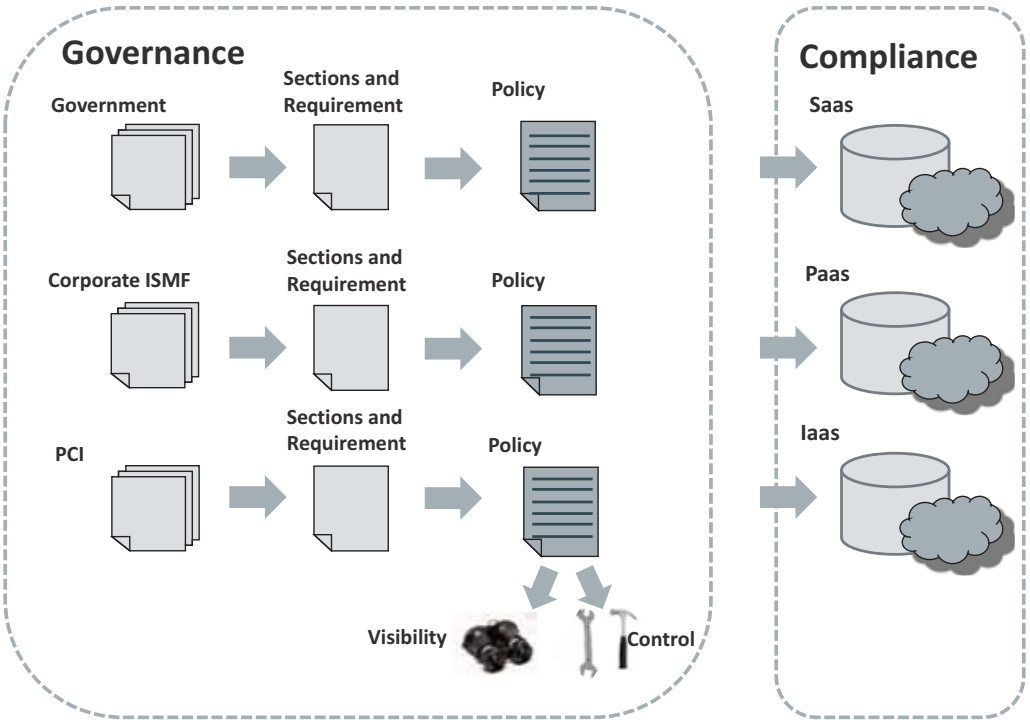
- Traditional strategies may not apply
- Move to the cloud requires new approaches
  - Transfer of risk to cloud provider?
  - Legal analysis of the liabilities?
  - Implications on information ownership & usage rights?
- Discussions on containment, segregation, monitoring & response, and a strong "right to audit" is needed

Enhanced Policies

- Policy framework need to go beyond traditional approaches
- Policies need to map each policy requirement with specific control requirements, and tied to business and/or regulatory requirements
- These enhanced policies provide clearer guidance in defining and managing the organisation's cloud security approaches

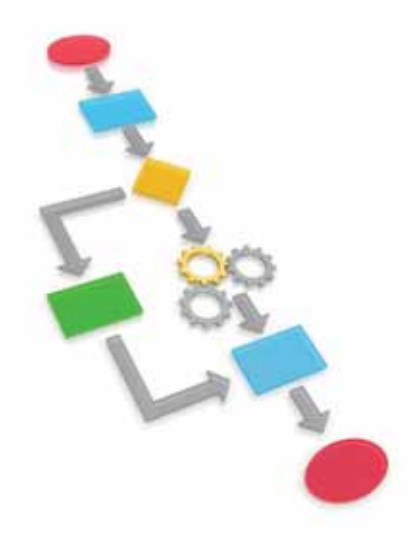


Enhanced Policies



Source: Adapted from Cloud Security Alliance (CSA)

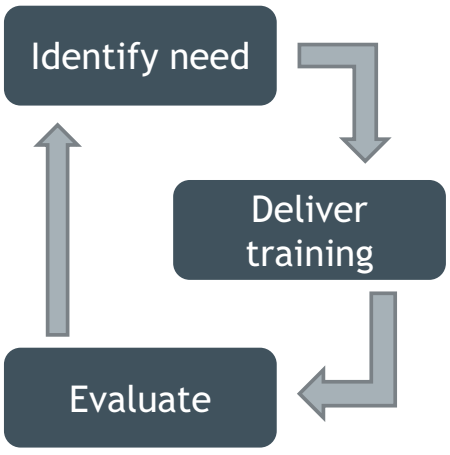
Formal Processes



- Adhoc processes will not do
- Decision methodology and risk management processes need to be clearly defined and understood
- Security practices need to be documented taking into consideration that direct infrastructure management may not be possible
- Visibility of the environment must be maintained with key metrics identified and tracked

Enhanced Training & Awareness

- Are current training programs appropriate?
- Define training objectives:
  - Connect people to the rationale and importance of enhanced policies and controls
  - Identify tie-in with daily responsibilities
  - Identify desired outcomes that improves decision making that have impact on security



Audit & Due Diligence

- Ask the right questions!
- Tie audit & quality management to specific requirements, assets & objectives

- Define items specifically to allow for improved visibility into practices
- How does the audit program allow your organisation to more effectively manage risk?

Ask the Right Questions

- What are the implications on information ownership & usage rights? Consider data location issues.
- What types of technical & non-technical controls are available to ensure data integrity & availability?
- What mechanisms are in place to ensure appropriate segregation?

Ask the Right Questions

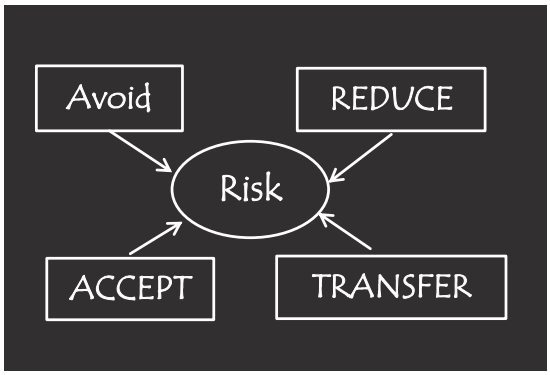
- What are the exit procedures & related costs? Consider data retention risks.
- How are security responsibilities defined?
- What monitoring & reporting mechanisms are available?

Ask the Right Questions

- Is there a right to audit? Or adequate audit coverage by 3rd party?
- What are the obligations between parties if things go wrong?
- Is there a formal plan to handle data security breaches?

Risk Assessment

- Identify risks
  - Legislative or regulatory
  - Compliance obligations
  - Multi-tenancy
  - Data security
  - Data ownership
  - Business continuity
  - Contractual agreements
- Vendor lock-in ➔ Data lock-in?



Vendor Selection

- Develop your checklist
- Use available guides and resources wherever applicable
  - NIST 800-144, 145, 146
  - CSA Cloud Controls Matrix, Consesus Assessments Initiative, Security Guidance v3

Document the Plan

- Analysis of key business/IT transformations
- Development of the solution
- Conduct QA and testing
- Implementation steps
- Back-out measures

Get business agreement on the plan and associated risks

Moving Forward

- Understand the cloud, get expert advice if needed
- Analyse business requirements & IT capabilities
- Define a robust GRC program that considers cloud risks and concerns
- Know your data/know how to secure it
- Identify the risks & legal obligations
- Ask the right questions
- Select appropriate CSP
- Verify exit requirements

Thank you

Review our whitepapers at
www.senseofsecurity.com.au/research/it-security-articles

Recognised as Australia's fastest growing information security and risk management consulting firm through the Deloitte Technology Fast 50 & BRW Fast 100 programs

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au